Toppersnotes
Unleash the topper in you

Jammu & Kashmir

Prosecuting Officer

Jammu and Kashmir Public Services Commission (JKPSC)

Paper – 1 || Volume - 5

Information Technology Act, The Protection of Children from Sexual Offences Act, Prevention of Corruption Act & Transfer of Property Act

SIERRA INNOVATIONS

INDEX

1 CHAPTER The Information Technology Act, 2000

Act No. 21 of 2000,

Date of enforcement: 17th October 2000

Date of enactment: 9th June, 2000

The Act's main purpose is:

1. **To legally recognize electronic transactions**
   - ✓ Earlier, contracts, agreements, and communications had to be on paper and signed physically.
   - ✓ This Act gave **legal validity** to transactions done through **electronic means** like emails, electronic data interchange (EDI), digital signatures, and online communication.
2. **To promote electronic commerce (e-commerce)**
   - ✓ It supports business activities carried out through the internet and other electronic networks.
   - ✓ It allows people and companies to **use digital records instead of paper-based documents**.
3. **To enable e-governance**
   - ✓ Citizens and businesses can file documents, applications, and forms electronically with government agencies.
   - ✓ This reduces dependency on physical paperwork.
4. **To update existing laws**
   - ✓ Since old laws were framed only for paper-based systems, the Act amended:
     - **Indian Penal Code (now BNS)** → to include crimes committed using computers and the internet.
     - **Indian Evidence Act, 1872 (Now BSA)** → to allow **digital evidence** (emails, digital records, etc.) in courts.
     - **Banker's Books Evidence Act, 1891** → to permit banks to keep and produce **electronic records** instead of paper ledgers.
     - **Reserve Bank of India Act, 1934** → to empower RBI to regulate and recognize electronic funds transfer, e-banking, etc.
5. **Other matters connected/incidental**
   - ✓ Covers areas like cybercrime, hacking, data protection, and misuse of electronic records.

CHAPTER - 1

Preliminary

Section 1 – Short Title, Extent, Commencement, and Application

1. **Short Title**
   - ✓ The Act is called the *Information Technology Act, 2000*.
2. **Extent**
   - ✓ It applies to the **whole of India**.
   - ✓ It also applies to **offences or contraventions committed outside India** by any person, provided they involve the provisions of this Act.
3. **Commencement**
   - ✓ The Act comes into force on a date notified by the Central Government.
   - ✓ Different provisions of the Act can come into force on **different dates** (flexibility in implementation).
   - ✓ Any reference to the commencement of the Act in a provision should be interpreted as the commencement date of that specific provision.
4. **Exemptions (Sub-section 4)**
   - ✓ The Act **does not apply** to certain documents or transactions listed in the **First Schedule**.
   - ✓ Examples in the First Schedule include:
     - Negotiable instruments (other than cheques)
     - Powers of attorney
     - Trust deeds
     - Wills and testamentary dispositions
     - Contracts for sale or transfer of immovable property
   - ✓ The **Central Government** has the power to **amend the First Schedule** by adding or deleting entries, via notification in the *Official Gazette*.
5. **Parliamentary Oversight (Sub-section 5)**
   - ✓ Every such notification made under sub-section (4) must be **laid before both Houses of Parliament** for transparency and oversight.

Section 2 – Definitions. – (1) In this Act, unless the context otherwise requires

(a) access with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

First understand the meaning of the two terms grammatical variations and cognate expressions.

1. **Grammatical variations**

   This means the different ways a word or phrase can change depending on grammar rules.
   - Example: The verb "run" changes as "runs, ran, running" → those are grammatical variations.
   - Another example: "child → children" (plural form).

   So basically: same word, different forms depending on tense, number, person, etc.

2. **Cognate expressions**

   "Cognate" means "related" or "having the same origin." Cognate expressions are words or phrases in different languages (or sometimes within the same language) that look or sound similar and often have the same meaning.
   - Example (English & Spanish): "family" and "familia" → they are cognates.
   - Example (English & French): "nation" and "nation."

   So basically: words in different languages that are like cousins because they come from the same root.

   In short:
   - Grammatical variations = different forms of the same word (runs, ran, running).
   - Cognate expressions = similar words across languages (family – familia).

Ingredients of this definition:

1. **Gaining entry** → Entering into a computer system/network (physically or remotely, e.g., logging in).
2. **Instructing** → Giving commands to the system (e.g., executing programs, running codes).
3. **Communicating with resources** → Interaction with the system's **logical, arithmetic, or memory functions**.
   - **Logical functions**: Operations based on logic (e.g., comparisons, conditions).
   - **Arithmetical functions**: Calculations performed by the computer.
   - **Memory functions**: Reading, writing, storing, retrieving data.

   "Access" basically means using or interacting with the internal functions of a computer or network—whether to enter, give instructions, or retrieve/modify data.

Practical Example

- ✓ **Accessing a website** → Communicating with a server.
- ✓ **Running software** → Instructing the logical/arithmetical functions.
- ✓ **Retrieving a file** → Accessing memory resources.
- ✓ **Unauthorized hacking** → Also counts as "access," even if done without permission.

This definition is very broad, it covers both authorized and unauthorized access, which is crucial for offences under the IT Act (e.g., hacking, data theft, unauthorized system entry).

(b) "Addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary.

Ingredients:

- ✓ **Addressee** = the person the message (electronic record) is meant for.
- ✓ **Originator** = the person who sends the message.
- ✓ **Intermediary** = someone who just passes the message along (like an email server, internet provider, or a messenger service).

An **addressee** is the *real intended receiver* of the message, **not** the middleman that helps deliver it.

(c) adjudicating officer means an adjudicating officer appointed under sub-section (1) of section 46;

(d) "affixing electronic signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

It means when you sign a physical paper, you use pen to prove "I approve this."

- ✓ In the **digital world**, you "sign" an electronic record using a digital signature, which is a cryptographic method that proves:
  - The document truly comes from you, and
  - It hasn't been altered after you signed it.

Thus, affixing an electronic signature is the digital equivalent of putting your handwritten signature on a physical document.

Ingredients:

"Any methodology or procedure" – It can be any recognized technical process (like asymmetric cryptography, Aadhaar-based e-sign, etc.).

"Authenticating an electronic record" – The purpose is to verify the signer's identity and document integrity.

"By means of digital signature" – The IT Act currently allows only methods that meet the definition of a **digital signature** under the Act (e.g., using a pair of public and private keys issued by a licensed Certifying Authority).

(da) Appellate Tribunal‖ means the Appellate Tribunal referred to in sub-section (1) of section 48;

(e) "Appropriate Government"

This term decides whether the **Central Government** or the **State Government** has authority over a particular matter under the IT Act.

- ✓ **If the matter is under:**
  1. **List II (State List)** of the 7th Schedule → **State Government** is the appropriate government.
  2. **List III (Concurrent List)** but concerning a **State law** → **State Government** again.
- ✓ **In all other cases** (like Union List matters, or general IT-related matters) → **Central Government** is the appropriate government.

Example:

- ✓ Regulation of police communication → State Government (State List).
- ✓ Cyber security policy → Central Government.

(f) "Asymmetric Crypto System"

This is the **technical system behind digital signatures**.

- ✓ It uses **two related keys**:
  1. **Private Key** – used by the sender to create (sign) a digital signature.
  2. **Public Key** – used by others to verify that the signature is genuine.

Example:

When you sign a document digitally, your private key encrypts the hash value; anyone can verify it using your public key.

Ensures both **authenticity** and **integrity** of the message.

(g) "Certifying Authority" (CA)

A **Certifying Authority** is an organization **licensed by the Controller of Certifying Authorities (CCA)** to issue **Digital Signature Certificates (DSCs)** or **Electronic Signature Certificates**.

- ✓ It verifies your identity before issuing a signature certificate.
- ✓ Only approved authorities can legally issue these certificates in India.

Example:

eMudhra, Sify, NIC, and (n)Code Solutions are licensed CAs in India.

(h) "Certification Practice Statement"

It's a formal **document issued by a Certifying Authority** describing how it operates and ensures security.

It specifies:

- ✓ Verification procedures before issuing certificates,
- ✓ How certificates are managed or revoked,
- ✓ Technical and security standards followed.

Example:

Before issuing your DSC, the CA must verify your identity per its **certification practice statement (CPS)**, ensuring reliability.

(ha) "Communication Device"

Added later through an amendment.

Means **any electronic device** used for **sending, receiving, or transmitting** text, video, audio, or images.

Examples:

- ✓ Mobile phones,
- ✓ Tablets,
- ✓ Laptops with communication apps,
- ✓ PDAs (Personal Digital Assistants).

Essentially, **any device used for digital communication**.

(i) "Computer"

A **computer** includes **any high-speed electronic or digital device** that performs logical, arithmetic, or memory operations using electronic, magnetic, or optical impulses.

Includes:

- ✓ CPU, monitor, keyboard (input/output devices),
- ✓ Storage units,
- ✓ Software and communication components connected to it.

Example:

A desktop PC, laptop, or server — all are "computers" under this Act.

(j) "Computer Network"

A **computer network** is a setup where **two or more computers or communication devices are interconnected** for sharing data or resources.

- ✓ Can be connected via:
  - Satellite, microwave, wire, wireless, or any medium.
- ✓ The connection can be continuous or temporary.

Example:

- ✓ Internet,
- ✓ Office LAN (Local Area Network),
- ✓ Wi-Fi-connected systems.

(k) "Computer Resource"

A broad term that includes **everything digital** in a computer ecosystem:

Computer, **Computer system**, **Computer network**, **Database**, **Software**, and **Data**.

Example:

If someone hacks into your e-mail or damages your software, they've tampered with a "computer resource."

(l) "Computer System"

A **computer system** means a **device or group of connected devices** (including input and output devices) that:

- ✓ Contains **computer programs** and **electronic instructions**,
- ✓ Can process **input data** and produce **output data**,
- ✓ Performs functions such as **logical operations, arithmetic operations, data storage, retrieval, and communication control**.

Excludes:

- ✓ **Calculators that are not programmable** (i.e., simple calculators that can't store programs or process external data).

In simple words:

A computer system is a **complete setup** that can **process, store, and communicate information**, not just a single machine.

Examples:

- ✓ Your **desktop computer** connected with a monitor, keyboard, and printer.
- ✓ A **bank's server setup** with terminals and data storage systems.
- ✓ **ATM network system** processing transactions.

(m)"Controller"

"Controller" means the **Controller of Certifying Authorities (CCA)**, appointed under **Section 17(1)** of the IT Act.

Role of the Controller:

- ✓ Supervises and regulates all **Certifying Authorities (CAs)** that issue **digital signature/e-sign certificates**.
- ✓ Ensures **trust, security, and legal compliance** in the digital signature ecosystem.
- ✓ Has power to **suspend or revoke** a CA's license if rules are violated.

Example:

The **Controller of Certifying Authorities (CCA)** under the **Ministry of Electronics and Information Technology (MeitY)** is the national authority for certifying authorities in India.

(na) "Cyber Café"

A **cyber café** is **any public facility** where **internet access is provided** to the public **in the ordinary course of business** (usually for a fee).

Examples:

- ✓ Local computer shops offering internet browsing or printing services.
- ✓ Public browsing centers where people access e-mails, online forms, or social media.

Note:

Under the **IT (Guidelines for Cyber Café) Rules, 2011**, owners must maintain **user identification records** and **system usage logs** for security and traceability.

(nb) "Cyber Security"

Protection of all digital assets — data, devices, computers, networks — from **unauthorized access, misuse, modification, or destruction**.

The purpose is to keep information safe and systems functioning properly.

Example: Firewalls, antivirus software, and encryption used by banks to protect customer data.

(o) "Data"

Any **representation of information or facts** that a computer can process.

It may exist as text, numbers, images, or sound and can be stored in many forms — **printouts, disks, magnetic or optical media, tapes**, etc.

Example: A spreadsheet of exam results or a scanned document stored on a hard drive.

(p) "Digital Signature"

A **method of authenticating an electronic record** using a cryptographic process described in **Section 3** of the IT Act.

It proves:

1. The identity of the sender, and
2. That the document hasn't been altered.
3. **Example:** Signing a PDF using your Digital Signature Certificate (DSC).

(q) "Digital Signature Certificate (DSC)"

An electronic certificate issued under **Section 35(4)** by a licensed **Certifying Authority** to confirm a person's identity for digital transactions.

Example: The DSC you use to sign income-tax or MCA e-forms.

(r) "Electronic Form"

Information that exists or is stored in **digital media**—magnetic, optical, computer memory, microfilm, or similar devices.

Example: A Word file, a scanned image, or a PDF on your computer.

(s) "Electronic Gazette"

The **Official Gazette** of the Government published **digitally** (instead of print).

Example: e-Gazette notifications on government websites.

(t) "Electronic Record"

Covers **all digital data or records**, including text, images, or sounds that are created, sent, received, or stored electronically.

Example: An e-mail, digital photograph, or online transaction log.

(ta)"Electronic Signature"

Any approved **electronic technique** (listed in the Second Schedule) used to authenticate an electronic record — **includes digital signature** but can cover newer methods (like Aadhaar e-sign).

Example: Aadhaar-based e-Sign used on government portals.

(tb)"Electronic Signature Certificate"

A certificate issued under **Section 35** that validates an **electronic signature**, including a **digital signature certificate**.

Example: The certificate behind your e-Sign authentication.

(u) "Function" (of a Computer)

Refers to all operations a computer can perform — **logic, arithmetic, deletion, storage, retrieval, and communication**.

Example: A computer calculating totals, deleting a file, or sending an e-mail.

(ua) "Indian Computer Emergency Response Team (CERT-In)"

An agency created under **Section 70B(1)** to act as the **national nodal agency for cyber-security incidents**.

Example: CERT-In handles hacking, phishing, and malware attack alerts in India.

(v) "Information"

Includes **data, messages, text, images, sound, voice, software, databases**, or any content stored in digital or microfilm form.

Example: A WhatsApp message or a database of voter records.

(w) "Intermediary"

Any person or company that **receives, stores, transmits, or provides a service** for another person's electronic records.

Includes **telecom operators, ISPs, web-hosting sites, search engines, payment gateways, e-commerce platforms**, and even cyber cafés.

Example: YouTube, Amazon, or Airtel — they act as intermediaries between users.

(x) "Key Pair"

A matched set of two mathematically linked keys in **asymmetric cryptography**:

- ✓ **Private Key** → used to create a digital signature.
- ✓ **Public Key** → used to verify it.
- ✓ **Example:** The pair used when you digitally sign a document.

(y) "Law"

Covers **all valid legal instruments** — Acts of Parliament or State Legislatures, Ordinances, Presidential Regulations, President's Acts under Art. 357, and any rules, bye-laws, or orders made under them.

(z) "Licence"

The official **authorization granted under Section 24** to a **Certifying Authority** to issue digital/e-signature certificates.

(za) "Originator"

The **person who creates or sends an electronic message** to another person, but **not an intermediary**.

Example: If you send an e-mail, you are the originator; Gmail is only the intermediary.

(zb) "Prescribed"

Means specified or laid down by **rules made under this Act** by the appropriate government.

(zc) "Private Key"

The **secret part** of a key pair used to **create a digital signature**.

It must be kept confidential by the owner.

Example: When you sign an e-file, your private key encrypts the document's digital hash.

(zd) "Public Key"

- ✓ It is the **second part of a key pair** in an asymmetric crypto system.
- ✓ The **public key** is used to **verify a digital signature** that was created using the corresponding **private key**.
- ✓ This key is **listed in the Digital Signature Certificate (DSC)** issued to a subscriber.

Example:

When you digitally sign a file with your private key, others can check its authenticity using your public key (which is publicly available through your DSC).

(ze) "Secure System"

A system (hardware, software, and procedures) that meets all these conditions:
(a) It is **reasonably safe** from unauthorized access or misuse.
(b) It works **reliably and correctly**.
(c) It is **fit for its intended purpose**.
(d) It **follows accepted security standards and practices**.

Example:

An e-governance portal that uses encryption, access control, and audit logs is a **secure system**.

(zf) "Security Procedure"

Refers to the **security measures prescribed by the Central Government under Section 16** of the Act.

These ensure the integrity, confidentiality, and authenticity of electronic records and signatures.

Example: Rules for digital signature verification or encryption standards notified by MeitY.

(zg) "Subscriber"

A **person in whose name an electronic-signature or digital-signature certificate is issued**.

This person is legally responsible for the use of the private key linked to that certificate.

Example:

If you obtain a DSC from eMudhra, **you** are the subscriber.

(zh) "Verify" (Check)

In relation to a **digital signature**, **electronic record**, or **public key**, "verify" means to check:

(a) Whether the electronic record was signed using the **private key** corresponding to the subscriber's **public key**; and
(b) Whether the record has remained **intact and unaltered** since the digital signature was applied.

Example:

When someone opens your digitally signed PDF, their computer uses your public key to verify that the file was indeed signed by you and not changed afterward.

Sub-section (2): Reference to Corresponding Law

If this Act mentions any **law or enactment** that is **not in force in a particular area**, it should be understood as referring to the **corresponding law in force in that area**.

Purpose:

To make the IT Act applicable even in regions where a particular central or state enactment is not yet operational, by linking it to an equivalent law there.

Section 3: Authentication of Electronic Records

(1) Authentication by Digital Signature

- ✓ Any **subscriber** (the person to whom a digital-signature certificate has been issued) can **authenticate an electronic record** by **affixing his digital signature** to it.
- ✓ This digital signature serves the same purpose as a **handwritten signature** on a physical document — it confirms the sender's identity and intent.

Example:

When you digitally sign an income-tax return (ITR) form before uploading it online, you are authenticating it under Section 3(1).

(2) How Authentication Works — Asymmetric Crypto System + Hash Function

The authentication process uses two core technologies:

(a) Asymmetric Crypto System

- ✓ Involves a **key pair**:
  - A **private key** (known only to the subscriber) — used to **sign** the document.
  - A **public key** (accessible to everyone) — used to **verify** the signature.

(b) Hash Function

- ✓ A **mathematical algorithm** that converts any electronic record into a **unique fixed-length string** called a **hash value** (or "hash result").
- ✓ The digital signature is applied to this hash, not to the full document — making the process secure and efficient.

Purpose of the Hash Function:

1. The same input always gives the **same hash result**.
2. It is **computationally infeasible** to:
   (a) Reconstruct the original file from its hash, or
   (b) Find two different files with the same hash result (collision-free).

Example:

If you digitally sign a PDF, a hash value of that PDF is first created → your private key encrypts that hash → the receiver uses your public key to decrypt and check the hash → if the hashes match, authenticity and integrity are confirmed.

(3) Verification Using the Public Key

- ✓ Anyone can verify the authenticity of a digital signature by using the **public key** of the subscriber.

- ✓ If the decrypted hash (from the signature) matches the recomputed hash (from the document), it proves:
- ✓ The document was signed by the rightful owner, and
- ✓ The document hasn't been changed since signing.

(4) Uniqueness of Key Pair

- ✓ Each subscriber has a **unique pair** of **private and public keys**.
- ✓ Together, they form a **functioning key pair** for secure communication and authentication.

Section 3A – Electronic Signature

This section extends authentication beyond *digital* signatures to include **any reliable electronic authentication technique** approved by the Government.

(1) Use of Electronic Signature

- ✓ Even if Section 3 talks about *digital signatures*, a subscriber may instead use **any electronic signature or authentication technique** that—
  (a) is **considered reliable**, and
  (b) is **listed in the Second Schedule** of the Act.

Thus, both *digital* and other *electronic* signatures (like Aadhaar e-Sign) are legally valid.

(2) When an Electronic Signature Is "Reliable"

An electronic signature is deemed **reliable** only if it meets all these five conditions

Clause	Requirement	Meaning in Simple Words
(a)	Signature / authentication data are linked uniquely to the signatory	The signature must belong to one identifiable person only
(b)	Signature data were under the signatory's exclusive control when signing	No one else could have used or accessed the signing key
(c)	Any alteration to the electronic signature after signing is detectable	Tampering with the signature can be discovered
(d)	Any change in the signed data after authentication is detectable	The system will show if the document was edited post-signature
(e)	Meets other prescribed technical / security standards	Central Govt can add extra reliability conditions

If these are satisfied, the signature is *legally trustworthy* and admissible as proof of identity and consent.

(3) Verification Procedure

- ✓ The **Central Government** may **prescribe the procedure** to verify whether an electronic signature truly belongs to the claimed person.
- ✓ This ensures a uniform national verification process (e.g., Aadhaar-based OTP or biometric check).

(4) Updating the Second Schedule

- ✓ The **Central Government** can, through notification in the **Official Gazette**,
  - **add or remove** an electronic-signature method, and
  - specify the **procedure** for affixing it.
- ✓ **Proviso:** No technique may be added unless it is proven *reliable* under clause (2).

(5) Parliamentary Oversight

- ✓ Every such Government notification must be **laid before both Houses of Parliament**, ensuring democratic scrutiny.

Illustration

Situation	**Example**
Government-approved e-signature	**Aadhaar e-Sign** (OTP or biometric-based) used for Income-Tax filings
Reliable features	Unique to user, controlled by user, detects alteration, traceable
Authority adding new method	MeitY (Central Govt) via Gazette notification updates the Second Schedule

This section gives legal recognition to all **reliable electronic authentication methods**, not just digital signatures.

It ensures **security, exclusivity, and tamper detection**, with Government control over approval and verification procedures.